Annals of Pure and Applied Logic 45 (1989) 211–225
North-Holland

FIRST-ORDER DEFINABILITY ON FINITE STRUCTURES

M. AJTAI
IBM Almaden Research Center, 650 Harry Road, San Jose, CA 95120-6099, USA

Communicated by Y. Gurevich

If k is a fixed positive integer, G is a graph with n vertices, $v_1, v_2 \in G$ then the property $d_G(v_1, v_2) \leq k$ can be easily defined by a first-order formula with at most $2 + 2\log_2 k$ quantifiers. Let M be a finite structure with n elements. We may consider G as a binary relation on the universe M. Using the relations of M may help to define the given property of G. (E.g. the number k may be coded by one of the relations.) However, we prove that if n is sufficiently large compared to k, then the given property cannot be defined by a first-order formula whose length does not depend on k even if we are allowed to use in this formula the arbitrary relations given on M. This result implies that the existential first-order formulas form a nontrivial hierarchy on finite structures in a strong sense.

Introduction

We say that P is a property defined on the subsets of finite structures if for every finite structure M and $A \subseteq M$, $P(A)$ is either true or false. E.g. "$|A|$ is even", or "$|A| = |M|/2$" are properties. We will also consider properties of binary relations, that is subsets of $M \times M$. E.g. "the graph defined by A is connected" is a property of the binary relation A. We will consider properties defined by first-order formulas. Let L be a first-order language and let $\mathscr{A}$ be a binary relation symbol not contained in L and $L' = L \cup \{\mathscr{A}\}$. Suppose now that π is an interpretation of the language L on the structure M. Let S^{π}_{ϕ} be the set of those binary relations A on M which satisfy the formula ϕ if we extend the interpretation π by $\mathscr{A} \to A$.

Assume now that a property P is given. We will be interested finding a ϕ so that at least for some interpretation π we have $P(A)$ iff $A \in S^{\pi}_{\phi}$. We may have relation symbols different from $\mathscr{A}$ in the formula ϕ. These relations (the so called built in relations of the structure) may actually help to define a property. E.g. it is proved in [1] that the property $|A| = [\log |M|]$ can be defined in the above sense by a first-order formula using built in relations. On the other hand this clearly cannot be done without built in relations. The question of definability without built in relations was studied by Fagin [2]. For a fixed first-order ϕ and an interpretation π, if the cardinality of the underlying set M is sufficiently large compared to the length of ϕ, then the set S^{π}_{ϕ} has a special combinatorial structure (cf. [1, Theorem 1.4]). As a consequence, it cannot be for example, the set of all even subsets, so "$|A|$ is even" cannot be defined by a first-order formula. This fact was also proved independently in [3] formulated in the language of constant

depth polynomial size Boolean circuits. (For the connection between the two cf. [4]).

We will say that a property P can be described by a first-order formula if there is a first-order formula ϕ so that for each positive integer t there is an interpretation π of the language L with an underlying set of size at least t so that for all binary relations A on the underlying set we have $P(A)$ iff $A \in S^{\pi}_{\phi}$. The mentioned result states that "$|A|$ is even" cannot be described by a first-order formula.

In this paper we show that another, in some sense simpler property of $A \subseteq M \times M$ is not first-order definable. Let $f(n)$ be a function which tends to infinity arbitrarily slowly as n tends to infinity and suppose that in all structures we have two fixed points v_1, v_2. Then the property $d_A(v_1, v_2) \leqslant f(|M|)$ cannot be described by a first-order formula, where d_A is the graph whose set of edges is A. (The results of [1] and [3] imply a similar statement only for a fixed function $f(n)$.)

The property $d_A(v_1, v_2) \leqslant f(n)$ is in some sense simpler than, e.g. the parity of $|A|$, since it can be defined by an existential first-order formula containing only $f(n)$ existential quantifiers. Therefore our theorem implies that the existential formulas form a nontrivial hierarchy according to the number of quantifiers and for all k there is an existential formula which is not equivalent to any first-order formula containing at most k quantifiers. (Actually $d_A(v_1, v_2) \leqslant f(n)$ can be defined by at most $2 + 2 \log_2 f(n)$ quantifiers.)

We will actually prove a slightly stronger statement. Suppose that $M_0, M_1, \ldots, M_{f(n)}$ are disjoint sets and for each $i = 0, 1, \ldots, f(n) - 1$, g_i is a one-to-one map of M_i onto M_{i+1}, $v_1 \in M_0$, $v_2 \in M_{f(n)}$, $M = \bigcup M_i$ and A is the set of pairs of the type $\langle a, g_i(a) \rangle$. We will prove that the property "$d_A(v_1, v_2) \leqslant f(n)$" which is equivalent to $g_{f(n)-1}(g_{f(n)-2}(\cdots g_0(v_1) \cdots)) = v_2$ cannot be described by a first-order formula. Here we are interested in the case when $f(n)$ is small compared to n. The other extreme is $f(n) = n/2$, $|M_i| = 2$ for $i = 1, \ldots, f(n)$. In this case the describability of $d_A(v_1, v_2) \leqslant f(n)$ is equivalent to the describability of parity. Indeed, if $M_i = \{a_i, b_i\}$ and $a_1 = v_1$, $a_{f(n)} = v_2$, then the inequality holds iff the number of g_i's with $g_i(a_i) = b_i$ is even.

Notation. $\mathcal{P}(X)$ is the power set of the set X; $\omega = \{0, 1, 2, \ldots\}$ is the set of all natural numbers; we consider the natural number n as the set $\{0, 1, \ldots, n-1\}$; $\mathrm{dom}(f)$ is the domain, $\mathrm{rng}(f)$ is the range of the function f; $f|_Y$ is the restriction of the function f to the set Y; $f''(Z)$ is the image of the set Z with respect to the function f.

1.

In the following we give a rigorous formulation of the mentioned results.

For all r, n let $l_n(r)$ be the smallest positive integer such that there is a

first-order formula $\varphi(A, \mathcal{R}_1, \ldots, \mathcal{R}_i, v_1, v_2)$ of length $l_n(r)$, (where A is a free second-order binary variable and $\mathcal{R}_1, \ldots, \mathcal{R}_i$ are relation symbols, v_1, v_2 are constant symbols) and an interpretation π of the language of ϕ (π interprets only the relation symbols of this language and not the variable A) on an underlying set M with n elements with the property:

$\forall A \subseteq M \times M$ if A is a graph, then $d_A(v_1, v_2) \leqslant r$ iff $\pi \vDash \phi(A)$.

Theorem 1. *If* $l(r) = \liminf_{n\to\infty} l_n(r)$, *then* $\lim_{r\to\infty} l(r) = \infty$. *That is the minimal necessary length for the definition of the property* $d(v_1, v_2) \leqslant r$ *tends to infinity with* r.

We actually prove the theorem in a stronger form. Suppose $f_0, \ldots, f_{r-1}$ are permutations of the set $m = \{0, 1, \ldots, m-1\}$. If our underlying set is $M = r \times (m \times m)$, then we may code f_i by a subset of $\{i\} \times (m \times m)$ and the whole sequence $f_0, \ldots, f_{r-1}$ by a subset of M.

Let us consider the following property.

(T1) $f_{r-1}(f_{r-2}(\cdots f_0(0 \cdots))) = 0$.

If we define $l'_m(r)$ as the minimal length of a formula ϕ which describes property (T1) on a suitable structure of size rm^2 in the same sense as in the case of $l_n(r)$, and $l'(r) = \liminf_{m\to\infty} l'_m(r)$, then we have:

Theorem 1′. $\lim_{r\to\infty} l'(r) = \infty$. *That is the minimal necessary length for defining the product of* r *permutations at a given place tends to infinity with* r.

Both Theorems 1 and 1′ imply the following:

Theorem 1″. *For all* k *there is an* r *and there is a* Σ_1 *formula* $\phi = \exists x_1, \ldots, x_r B(x_1, \ldots, x_r, R_1, \ldots, R_k, A)$ (*where* $R_1, \ldots, R_k$ *are relation symbols,* A *is a free second-order variable and* B *is a Boolean expression*) *so that for any interpretation* π *of* $R_1, \ldots, R_k$ *on a sufficiently large universe, there is no first-order formula* θ *with only* k *quantifiers and an extension* π' *of* π *with* $\forall A\ \pi \vDash \phi(A)$ *iff* $\pi' \vDash \theta(A)$.

We may consider the points of the underlying set $r \times (m \times m)$ as the edges of a graph whose set of vertices is the set $(r+1) \times m$. Indeed the element $\langle i, \langle s, t\rangle\rangle \in r \times (m \times m)$ corresponds to the edge which connects the points $\langle i, s\rangle$ and $\langle i+1, t\rangle$. In other words the points $\langle i, s\rangle\langle i+1, t\rangle$ will be connected by an edge iff $f_i(s) = t$. Hence (T1) holds in our graph if and only if $d(\langle 0, 0,\rangle, \langle r, 0\rangle) \leqslant r$. In a graph of this type, this inequality holds iff the two points are connected.

In the proofs we use a slightly different terminology, namely, we do not consider subsets of the underlying structure but functions defined on it.

Definition. If M is a finite set and F is a subset of ${}^M M$, then we say that the

first-order formula $\phi(X)$ (where X is a unary free variable) describes F, if there is an interpretation π of the language of ϕ, with the underlying set M, so that

$$\forall f \in {}^{M}M \quad f \in F \leftrightarrow \pi \vDash \phi(f),$$

M will always be the set $r \times m$, for some $r, m \in \omega$ and F will be the set of all functions $f \in {}^{M}M$ with the following properties:

(T2) For all $i \in r-1$, $f|_{\{i\}\times m}$ is a one-to-one map of $\{i\} \times m$ onto $\{i+1\} \times m$ (f may take arbitrary values on $\{r-1\} \times m$), and

(T3) $f^{r-1}(\langle 0,0\rangle) = f(f(\cdots f(\langle 0,0\rangle)\cdots)) = \langle r-1, 0\rangle$.

We want to prove that if $\phi(X)$ is fixed, then $\exists r_0 \forall r > r_0 \exists m_0 \forall m > m_0$ ϕ does not describe F on $r \times m$.

There is some similarity between our proof and the proof given in [1] but the combinatorial details are different. We do not suppose that the reader is familiar with the proof given there.

We will suppose that an underlying set M is fixed and we will consider the set H of those $f \in {}^{M}M$ which satisfy a first-order formula. Our goal is to show that if the length of the formula is constant while the size of the structure tends to infinity, then this set has some nontrivial combinatorial structure. The proof of the nondefinability of parity suggests that we may try to get the following type of result: if we randomly fix the values of a function f at all but $n^{\frac{1}{2}}$ places, then with high probability there will be a set of constant size T so that the values of f on T already decide whether f is in H or not. Unfortunately this is not true. We will actually prove a similar statement that we get from the above assertion with the following modifications.

(1) We will not consider all functions in ${}^{M}M$ but only those functions f which have the property described in (T2). That is H will be always a subset of this set of functions.

(2) We fix certain values of a function f randomly but the set of places where we assign a random value of the function will not be completely random. In fact we will take into account the structure of $r \times m$. For certain i's there will be a value assigned to the function everywhere, for others we will assign a value to each but $[n^{\epsilon}]$ points where $\epsilon > 0$ tends to 0 as the length of the formula tends to infinity. The set of those i's where we do not assign values everywhere will be the set of integers less than r and divisible by 2^k where k depends on the length of the formula. We will also have the additional assumption that there are $n - [n^{\epsilon}]$ points x of $\{0\} \times m$, so that $f^{r}(x)$ is defined, that is those places on the various levels $\{i\} \times m$ where f is defined are synchronized according to the paths defined by f.

(3) We will consider the values of not only f but also f^{-1} on the set T. That is we fix the values of a random f in the given way, then with high probability (greater than $1 - n^{-c}$) there will be a set of constant size T so that if we give the values of both f and the inverse of f on the set T then it decides whether the

function is in H. This will imply that H cannot be the set of all f with $f^{r-1}(\langle 0,0\rangle) = f(f(\cdots f(\langle 0,0\rangle)\cdots)) = \langle r-1, 0\rangle$. (We will prove that if we are going along the path defined by f and starting from $\langle 0,0\rangle$, then with a positive probability (greater than $1/n$) we will get to a point where f is not defined. At this point we will use the fact that $|T|$ is smaller than $r/2^k$ that is the number of i's where f is not defined on the whole $\{i\} \times m$.

First we give the basic definitions of the mentioned concepts.

Definition. Let L be an ordered finite set and W be an arbitrary finite set $M = L \times W$. Let 0_L be the least, 1_L be the greatest element of L. If x is an element of L, then $\bar{x}$ will be the smallest element of L which is greater than x.

Using our earlier notations let $r = L$, $m = W$. Func(L, W) will denote the set of all functions f which are defined on $(L - 1_L) \times W$, so that for all $x \in L - 1_L$ we have that $f|_{\{x\}\times W}$ is a one-to-one map of $\{x\} \times W$ onto $\{\bar{x}\} \times W$.

Obviously, $f^{|L|-1}$ maps $\{0_L\} \times W$ onto $\{1_L\} \times W$. Our chief aim is to show that the property $f^{|L|-1}(\langle 0_L, w_0\rangle) = \langle 1_L, w_0\rangle$ is not first-order definable where w_0 is an arbitrary but fixed element of W.

We define a hierarchy on the subsets of Func(L, W). The simplest type of subsets will be called cylinders.

Definition. An (L, W) cylinder C will be a subset of Func(L, W) of the form $C = \{f \in \text{Func}(L, W) \mid g \subseteq f\}$ where g is an arbitrary function which has at least one extension in Func(L, W). $g = b(C)$ will be called the base of the cylinder C and we will use the notation $\|C\| = |g|$.

We will construct the further levels of the hierarchy by taking unions of a polynomial number of sets on the previous levels or taking the complement of a set in a previous level. We also define a function w which measures how many sets were used altogether in the construction of a set at given level of the hierarchy.

Definition. If i, s are natural numbers $V_i^s(M)$ will be a subset of the power set of Func(L, W) and w_i a function defined on a set containing $V_i^s(M)$. For an arbitrary s let $V_0^s = \{C \mid C \text{ is an } (L, W) \text{ cylinder and } \|C\| = 1\}$, $w_0(H) = 1$ for all $H \in V_0^s$.

If i is even an $H \subseteq \text{Func}(L, W)$, then let

$$w_{i+1}(H) = \min\left\{\sum_{B\in G} w_i(B) \mid G \subseteq V_i^s \text{ and } H = \bigcup G\right\},$$

$$V_{i+1}^s = \{H \subseteq \text{Func}(L, W) \mid w_{i+1}(H) \leqslant s\}.$$

If i is odd,

$$V_{i+1}^s = \{H \subseteq \text{Func}(L, W) \mid H \in V_i^s \text{ or } \text{Func}(L, W) - H \in V_i^s\},$$

and for all $H \in V^s_{i+1}$,

$$w_{i+1}(H) = w_i(H) \quad \text{if } H \in V^s_i, \quad \text{and}$$

$$w_{i+1}(H) = w_i(\text{Func}(L, W) - H) \quad \text{if } \text{Func}(L, W) - H \in V^s_i.$$

If $\phi(X)$ is a first-order sentence with the unary function variable X, then let

$$S^\pi_\phi(L, W) = \{f \in \text{Func}(L, W) \mid \pi \vDash \phi(f)\}.$$

Lemma 1. (a) *If $\phi(X)$ is a first-order formula, then there are $i, j \in \omega$, so that for any L, W, π we have $S^\pi_\phi(L, W) \in V^{n^j}_i(L, W)$, where $n = |L||W|$ and π is an interpretation of ϕ on $L \times W$.*

(b) *Conversely, suppose $i, j \in \omega$. Then there exists a first-order sentence ϕ such that for all L, W and $H \in V^{n^j}_i(L, W)$, there exists an interpretation π with $H = S_\phi(L, W)$.*

This is the analogue of Lemma 1.1 of [1] and can be easily proved by induction on the number of quantifiers, and i.

As we mentioned earlier we will randomly fix certain values of f. This defines a partial function on $L \times W$. In the following definitions we describe those types of partial functions that we may get in this form.

Definition. $\text{fn}(L, W)$ will be the set of those functions g which have an extension in $\text{Func}(L, W)$. For each $g \in \text{fn}(L, W)$, let $\hat{g}$ be an arbitrary (but fixed) extension of g in $\text{Func}(L, W)$.

We define another set of functions $\text{fn}(L, W, s)$. A function in $\text{fn}(L, W, s)$ will be defined everywhere on certain sets of the type $\{y\} \times W$ and on all of the others it will be defined exactly at $|W| - s$ places. Moreover, we suppose that there is a restriction of the function, defined exactly at $|W| - s$ points on each $\{y\} \times W$, $y \neq 1_L$ and whose domain on $\{\bar{y}\} \times W$ coincides with its range on $\{y\} \times W$. More precisely $\eta \in \text{fn}(L, W, s)$ iff $\eta \in \text{fn}(L, W)$ and there exists a $g \in \text{fn}(L, W)$ so that for all $y \in L - \{1_L\}$, $\bar{y} \in L - \{1_L\}$ we have $\text{dom}(g|_{\{\bar{y}\} \times W}) = \text{rng}(g|_{\{y\} \times W})$, $|g|_{\{y\} \times W}| = |W| - s$, η is an extension of g and for all $y \in L - \{1_L\}$ either $\text{dom}(\eta|_{\{y\} \times W}) = \text{dom}(g|_{\{y\} \times W})$ or $\text{dom}(\eta|_{\{y\} \times W}) = \{y\} \times W$.

Suppose that H is a subset of $\text{Func}(L, W)$ which is defined by a first-order formula; that is $H \in V^{n^j}_i$ for some constants i, j. As we have indicated earlier we will randomly fix certain values of a function f. Let η be the partial function defined this way. We will suppose that $\eta \in \text{fn}(L, W, s)$. We will be interested in the set H' of those extensions of η which are in the set H. The following definitions show that this set can be considered as a subset of $\text{Func}(L^{(\eta)}, W^{(\eta)})$ for a suitably defined pair $L^{(\eta)}, W^{(\eta)}$, moreover the set H' will be on a lower level of the V hierarchy than H. We will also show that if H was defined as the set of functions f with $f^{r-1}(\langle 0, 0\rangle) = \langle r - 1, 0\rangle$ then the corresponding statement will be

true for H' in the new universe $L^{(\eta)}$, $W^{(\eta)}$. Thus using induction, we will reduce the original question to the special case when H is a cylinder.

In the following definitions we define the new (smaller) universe $L^{(\eta)}$, $W^{(\eta)}$, if η is given.

Before giving the exact definitions we sketch the definition of $L^{(\eta)}$, $W^{(\eta)}$. The partial function η defines a graph on the set $r \times m$ if we connect x and $\eta(x)$ for all x in the domain of η. Each connected component of this graph is a path. We will disregard those connected components which have exactly r elements. The set of the remaining connected components will be essentially $L^{(\eta)} \times W^{(\eta)}$. $L^{(\eta)}$ will be the set of those elements in L where η is not defined everywhere on $\{y\} \times W$. $W^{(\eta)}$ will be the set of all $x \in W$ such that starting a path from $\langle 0_L, x\rangle$ defined by $\hat{\eta}$ we go through a point where η is not defined. If we define $L^{(\eta)}$ and $W^{(\eta)}$ this way then there is a natural one-to-one correspondence between $L^{(\eta)} \times W^{(\eta)}$ and the set of connected components with fewer then r elements.

Definition. If $\eta \in \mathrm{fn}(L, W, s)$, then let $L^{(\eta)}$ be the set of all $y \in L$ with $|\mathrm{dom}(\eta|_{\{y\}\times W})| = |W| - s$ or $y = 1_L$. $W^{(\eta)}$ will be the subset of W defined by $x \in W^{(\eta)}$ iff there exists an $i \in \{0, 1, \ldots, |L| - 2\}$ such that $\hat{\eta}^i(\langle 0_L, s\rangle) \notin \mathrm{dom}(\eta)$. If η is not total, then $|W^{(\eta)}| = s$. The set $L^{(\eta)} \times W^{(\eta)}$ has a natural embedding $R(\eta)$ into $L \times W$, described below.

If $\langle y, x\rangle \in L^{(\eta)} \times W^{(\eta)}$, then $R(\eta)(\langle y, x\rangle) = \hat{\eta}^i(\langle 0_L, x\rangle)$ where $i = |\{z \in L \mid z < y\}|$. (Thus $R(\eta)(\langle y, x\rangle) = \langle y, w\rangle$ for a suitable $w \in W$.) We note that η is not defined exactly on $R(\eta)''(L^{(\eta)} \times W^{(\eta)}) \cup (1_L \times W)$ (from the points of $L \times W$).

If $f \in \mathrm{fn}(L, W)$ and f is compatible with η (that is their union is in $\mathrm{fn}(L, W)$), then let $f_\eta \in \mathrm{fn}(L^{(\eta)}, W^{(\eta)})$ where $f_\eta(u)$ is defined if and only if $(R(\eta))(u) \in \mathrm{dom}(f)$, and in this case $f_\eta(u) = (R(\eta)^{-1})(\hat{\eta}^i(f(R(\eta)(u))))$ where i is the smallest nonnegative integer with $\hat{\eta}^i(f(R(\eta)(u))) \in \mathrm{rng}(R(\eta))$.

If $F \subseteq \mathrm{fn}(L, W)$, then $F_\eta = \{f_\eta \mid f \in F, f \text{ and } \eta \text{ are compatible}\}$. If $X \subseteq L \times W$, then $X_\eta = (R(\eta))^{-1}(X)$. We will use later the following important fact: if $\eta \in \mathrm{fn}(L, W, s)$ and $h \in \mathrm{Func}(L^{(\eta)}, W^{(\eta)})$, then there exists exactly one $f \in \mathrm{Func}(L, W)$ so that $f \supseteq \eta$ and $f_\eta = h$.

If C is an (L, W) cylinder with $b(C) = \eta$, then for each $A \subseteq \mathrm{Func}(L, W)$, let $\tilde{A}_C = A_\eta$.

A set T of (L, W) cylinders will be called (s, q)-complete if $\bigcup T = \mathrm{Func}(L, W)$, the elements of T are pairwise disjoint and, for all $C \in T$, C is an (L, W) cylinder, $b(C) \in \mathrm{fn}(L, W, s)$ and $|L^{(\eta)}| = q$, $|W^{(\eta)}| = s$, where $\eta = b(C)$.

2.

The following lemma contains an assertion about the combinatorial structure of the sets at low levels of the V_i^n hierarchy (i, j are constant and n is sufficiently large). As we will explain after the statement of the Lemma this assertion implies

our nondefinability results. The lemma itself essentially states that if $A \in V_i^{n^j}$ then it is possible to partition Func(L, W) into a set of not too small (L, W) cylinders so that inside almost all cylinders, A will be the union of cylinders whose bases are of constant size. Moreover, this assertion holds for a polynomial number of A's simultaneously.

Lemma 2. *For all* $e, i, j, d \in \omega$ $\exists t \in \omega$, $\epsilon > 0$, $\forall q\ \exists r_0\ \forall r > r_0\ \exists m_0\ \forall m > m_0$, *if* $|L| = r$, $|W| = m$ *and* $\mathcal{A} \subseteq V_i^{n^j}$, *(where* $n = |L|\,|W|$*),* $|\mathcal{A}| < n^e$, *then there exists a* $([n^\epsilon], q)$*-complete set* T *of* (L, W) *cylinders, so that for almost all* $D \in T$ *(with a probability greater than* $1 - n^{-d}$*), we have: if* $A \in \mathcal{A}$, *then* $\tilde{A}_D = \bigcup_{C \in B} C$, *where* B *is a set of* $(L^{(\eta)}, W^{(\eta)})$ *cylinders (where* $\eta = b(D)$*) and* $C \in B$ *implies* $\|C\| \leq t$.

First we show how the nondefinability of $f^{|L|-1}(\langle 0_L, w_0\rangle) = \langle 1_L, w_0\rangle$ follows from this lemma. We have to prove that $\forall i, j \in \omega\ \exists r_0 \forall r > r_0 \exists m_0 \forall m > m_0$ if $|L| = r$ and $|W| = m$, then

$$F = \{f \in \text{Func}(L, W) \mid f^{|L|-1}(\langle 0_L, w_0\rangle) = \langle 1_L, w_0\rangle\} \notin V_i^{n^j}.$$

Let us define for each $u, v \in W$,

$$F_{u,v} = \{f \in \text{Func}(L, W) \mid f^{|L|-1}(\langle 0_L, u\rangle) = \langle 1_L, v\rangle\}.$$

$F \in V_i^{n^j}$ would imply $F_{u,v} \in V_i^{n^j}$ (since the definition of $V_i^{n^j}$ is symmetric on each $\{i\} \times W$). So we have that for some $x, y \in W^{(\eta)}$, $F_{x,y} = \bigcup_{C \in B} C$ (where $F_{x,y}$ is defined on $L^{(\eta)} \times W^{(\eta)}$), where $C \in B \rightarrow \|C\| \leq t$, which is clearly impossible since $F_{x,y}$ cannot contain any $(L^{(\eta)}, W^{(\eta)})$ cylinders C with $\|C\| < |L^{(\eta)}| - 1$.

We prove Lemma 2 through the following lemma. This lemma essentially states the same as Lemma 2 for the special case when each each $A \in \mathcal{A}$ is the complement of a union of cylinders with bases of constant size. This lemma will make possible an inductive proof of Lemma 2, where the induction will be on i (the number of levels in the V hierarchy).

Lemma 3. $\forall e, d, t' \in \omega\ \exists \epsilon > 0$, $t \in \omega\ \forall q\ \exists r_0\ \forall r > r_0\ \exists m_0\ \forall m > m_0$ *if* $|L| = r$, $|W| = m$, $\mathcal{A} \subseteq \mathcal{P}(\text{Func}(L, W))$, $|\mathcal{A}| \leq n^e$ *and* $\forall A \in \mathcal{A}\ A = \bigcup_{C \in X_A} C$ *where* X_A *is a set of cylinders with* $C \in X_A \rightarrow \|C\| \leq t'$, *then there exists a* $([n^\epsilon], q)$*-complete set* T *of cylinders such that for almost all (with a probability greater than* $1 - n^{-d}$*)* $D \in T$, *we have that for all* $A \in \mathcal{A}$ *if* A' *is the complement of* A *in* Func(L, W), *then* A *satisfies the following condition*:

(P1) $\tilde{A}'_D = \bigcup_{C \in B} C$

where B *is a set of* $(L^{(b(D))}, W^{(b(D))})$ *cylinders and* $C \in B \rightarrow \|C\| \leq t$.

We start the proof of this lemma by a simple but basic definition. Till now we have used $\|C\|$, that is, the size of $b(C)$, as the measure of complexity for a cylinder. This notion however is not really suitable for this purpose if we have a set of cylinders. E.g. it is possible that all cylinders in a set have bases of constant

size, but still the complement of the union of these cylinders is not the union of cylinders with constant norms (even if we allow here a greater constant). We will be able to handle the complement of a union of cylinders if we suppose that the original cylinders were all concentrated on a single set H of constant size, in a sense explained in the following definition and property (P2).

Definition. If $g \in \mathrm{fn}(L, W)$ and $H \subseteq L \times W$, we say that H covers g if for all $x \in \mathrm{dom}(g)$ either $x \in H$ or $g(x) \in H$.

We will prove Lemma 3 with a property (P2) defined below, instead of property (P1), and prove that property (P2) implies property (P1).

(P2) $\tilde{A}_D = \bigcup_{C \in B} B$ *where* B *is a set of* $(L^{(b(D))}, W^{(b(D))})$ *cylinders, and there is a* $H \subseteq L^{(b(D))} \times W^{(b(D))}$ *so that* $|H| \leq t$ *and* H *covers* $b(C)$ *for all* $C \in B$.

First we prove that (P2) implies (P1). If $f \in \tilde{A}'_D$ then $f \notin \tilde{A}_D$. Let $H_f = \{x \mid x \in H \text{ or } f(x) \in H\}$ and let C_f be the cylinder with $b(C_f) = f|_{H_f}$ (where H is from (P2)). Obviously, $f \in C_f$ and $\|C\| \leq 2|H| \leq 2t$. In order to prove $\tilde{A}'_D = \bigcup C_f$, we have to show that $C_f \subseteq \tilde{A}'_D$, that is, $C_f \cap \tilde{A}_D = \emptyset$. Indeed, if $g \in A_D$, then by (P2) there is a cylinder $C \subseteq \tilde{A}$, so that $g \in C$ and H covers $b(C)$. $f \in \tilde{A}'_D$ implies that $f \notin C$, that is, f and $b(C)$ are incompatible. Hence, there are x, y with $y = (b(C))(x)$, $y \neq f(x)$ and $x \in H$ or $y \in H$. If $x \in H$, then $x \in H_f$; if $y \in H$, then there is a $z \in H_f$ with $y = f(z)$. In both cases, $f|_{H_f}$ is incompatible to $b(C)$, that is, $C_f \cap C = \emptyset$, $C_f \cap \tilde{A}_D = \emptyset$.

In the following Lemma 4 we reformulate the statement Lemma 3 (with (P2) instead of (P1)), so that we are speaking only about the bases of the cylinders.

Definitions. (1) $\mathrm{fn}(L, W, S, q) = \{\eta \in \mathrm{fn}(L, W, s) \mid |L^{(\eta)}| = q\}$.

(2) A subset Γ of $\mathrm{fn}(L, W)$ is called complete on $L \times W$ if for each $f \in \mathrm{Func}(L, W)$, there is exactly one $g \in \Gamma$ with $f \supseteq g$.

(3) If $F \subseteq \mathrm{fn}(L, W)$, then $w(F) = \min\{|H| \mid \forall f \in F\ H \text{ covers } f\}$.

Lemma 4. $\forall e, d, t' \in \omega\ \exists \epsilon > 0,\ t \in \omega\ \forall q\ \exists r_0\ \forall r > r_0\ \exists m_0\ \forall m > m_0$ *if* $|L| = r$, $|W| = m$ *and* $\mathcal{F}$ *is a set of subsets of* $\mathrm{fn}(L, W)$ *with* $|\mathcal{F}| \leq n^e$, $F \in \mathcal{F} \to \|F\| \leq t'$ *(i.e., for all* $f \in F\ |f| \leq t'$*), then there is a complete set of functions* Γ *on* $L \times W$ *with* $\Gamma \subseteq \mathrm{fn}(L, W, s, q)$, $s = [n^\epsilon]$ *so that for almost all* $\eta \in \Gamma$ *(with a probability greater than* $1 - n^{-d}$*), we have: for each* $F \in \mathcal{F}\ w(\mathrm{Min}(F_\eta)) \leq t$ *where* $\mathrm{Min}(G) = \{g \in G \mid \forall h \in G - \{g\}\ h \not\subseteq g\}$.

If $\mathcal{F} = \{F_A \mid F_A = \{b(C) \mid C \in X_A, A \in \mathcal{A}\}\}$, ($\mathcal{A}, X_A$ as in Lemma 3), then we get that for almost all D where $b(D) \in \Gamma$, $A \in \mathcal{A}$ implies that $\tilde{A}_D = \bigcup_{C \in B} C$ where $B = \{C \mid C \text{ is an } (L^{b(D)}, W^{b(D)}) \text{ cylinder, } b(C) \in \mathrm{Min}((F_A)_{b(D)})\}$; hence we have (P2). We will give a random construction for Γ. We will define a random variable η whose possible values will be the elements of Γ.

We say that η is a Γ-random variable on $L \times W$ if there is an s and q so that the possible values of η are in $\mathrm{fn}(L, W, s, q)$ and form a complete set of functions on $L \times W$, and the distribution of η is uniform on its possible values.

To simplify our notations, we will suppose that L, W are the natural numbers r, m and $L^{(\eta)}$, $W^{(\eta)}$ will be identified with the natural numbers $r^{(\eta)} = q$, $m^{(\eta)} = s$.

Definitions. (1) If $F \subseteq \mathrm{fn}(r, m)$, then let

$$\|F\| = \max\{|f| \mid f \in F\}, \qquad \mathrm{Min}(F) = \{f \in F \mid \forall g \in F - \{f\}\, g \not\subseteq f\},$$
$$\mathrm{Min}_k(F) = \{f \in \mathrm{Min}(f) \mid |f| = k\}.$$

(2) Let A and B be unary relations defined on the set $\mathrm{Pr} = \{\langle r, m, F, t\rangle \mid r \in \omega, m \in \omega, F \subseteq \mathrm{fn}(r, m), t \in \omega\}$. We say that A can be reduced to B or $Q(A, B)$ if the following assertion holds: $\forall t' \in \omega\, \exists \epsilon > 0$, $c > 0$, $h \in {}^{\omega}\omega$ with $\lim_{x \to \infty} h(x) = \infty$, $\exists t_0 \in \omega\, \forall t > t_0\, \forall r \in \omega$ if $r > 1/c$ then for all sufficiently large $m \in \omega$, then there exists a Γ-random variable η on $r \times m$ whose values are in $\mathrm{fn}(r, m, [m^{\epsilon}])$ with $r^{(\eta)} > cr$, so that for all $F \subseteq \mathrm{fn}(r, m)$ we have

$$P(A(r, m, F, t') \to B(r^{(\eta)}, [m^{\epsilon}], \mathrm{Min}(F_\eta), t)) \geq 1 - m^{-h(t)}.$$

Lemma 4 follows immediately from the following assertion.

Lemma 5. *$\|F\| \leq t'$ can be reduced to $w(F) \leq t$.*

Indeed, suppose that Lemma 5 holds and $e, d, t' \in \omega$ are fixed. Lemma 5 and the definition of reducibility implies that there is an $\epsilon > 0$, $c > 0$, $h \in {}^{\omega}\omega$ with the properties given in the definition of reducibility, and now with the conclusion

$$P((\|F\| \leq t') \to (w(F) \leq t)) \geq 1 - m^{-h(t)}.$$

We pick the integer t of Lemma 4 so that $t > t_0$ and $h(t) > d + e$. r_0 can be any positive integer with $r_0 > 1/c$, and m sufficiently large compared to t', t, r. Assume that L, W, $\mathcal{F}$ are fixed with the properties listed in Lemma 4. Applying Lemma 5 we get the conclusion of Lemma 4.

For the proof of Lemma 5, we need a more specific version of the notion of reducibility.

Definition. Let A, B be unary relations on the set Pr defined earlier (definition of reducibility). Suppose $k \in \omega$; we say that A can be k-reduced to B or $Q_k(A, B)$, if the following assertion holds:

$\exists \epsilon > 0$, $c > 0$, $h \in {}^{\omega}\omega$ with $\lim_{x \to \infty} h(x) = \infty$ so that $\forall t' \in \omega\, \exists t_0 \in \omega\, \forall t > t_0\, \forall r \in \omega$ if $r > 1/c$, then for all sufficiently large $m \in \omega$, there exists a Γ-random variable η whose values are elements of $\mathrm{fn}(r, m, [m^{\epsilon}])$ with $r^{(\eta)} > cr$, so that for all $F \subseteq \mathrm{fn}(r, m)$, if $\|F\| \leq k$, then

$$P(A(r, m, F, t') \to B(r^{(\eta)}, [m^{\epsilon}], \mathrm{Min}_k(F_\eta), t)) \geq 1 - m^{-h(t)}.$$

The proof of Lemma 5 is based on the following combinatorial lemmas.

Lemma 6. *Suppose that* $0<\epsilon<\frac{1}{2}$, $0<\delta<\epsilon/4$ *and* g *is a function defined on the finite set* H *with* n *elements such that* $g(x)\subseteq H$, $|g(x)|\leq|H|^{1-\epsilon}$ *and* $x\neq g(x)$ *for all* $x\in H$. *If* $j<|H|^{\delta}$ *and* H' *is a random subset of* $|H|$ *with* j *elements, then for all* $t>0$ *we have*

$$P(|\{y \mid y\in H' \text{ and } y\in g(x) \text{ for some } x\in H'\}|\geq t)<n^{-c_1t+c_2}$$

where $c_1>0$ *and* c_1, c_2 *depend only on* ϵ.

We will use the following well-known fact of elementary combinatorics (or probability theory):

(*) Assume that A is a set of subsets of H with $|A|<|H|^d$, $|X|<|H|^{1-\epsilon}$ for all $X\in A$ and H_0 is a random subset of H with $[|H|^{\epsilon_1}]$ elements where $0<\epsilon_1<\epsilon$. Then

$$P(\forall X\in A\,|X\cap H_0|<k)>1-|H|^{-d_1k+d_2}$$

where $d_1>0$ and d_1, d_2 depend only on d, ϵ_1, ϵ.

(*) can be proved by giving first an estimate of the corresponding probability for an arbitrary but fixed $X\in A$. We may get this by counting for all $i\geq k$ the number of sets of the form $X\cap H_0$ with i elements (this is simply the number of i-tuples in X), then for each fixed such set the number of all corresponding sets H_0 (this is the number of $[|H|^{\epsilon_1}]-i$-tuples in $H-X$).

We need also another assertion of similar type which can be proved easily by a counting argument:

(**) If $|H|$ is a set with n element and for each $x\in H$ we have $Q(x)\subseteq H$, $|Q(x)|\leq t$, $x\notin Q(x)$ and H' is a random subset of H with $[|H|^{(1/2)-\epsilon}]$ elements, then

$$P(|\{x\in H' \mid \exists y\in H'\, x\in Q(y)\}|\geq t)\leq n^{-c_3t+c_4}$$

where $c_3>0$ and c_3, c_4 depend only on ϵ

Proof of Lemma 6. Let us choose a random subset $H_0\subseteq H$, then a $H_1\subseteq H_0$ and $H_2\subseteq H_1$ with $|H|^{\epsilon_0}$, $|H|^{\epsilon_1}$, $|H|^{\epsilon_2}$ elements where $\epsilon_0<\epsilon$, $\epsilon_1<\epsilon_0/2$, $\epsilon_2<\epsilon_1/2$.

Throughout the proof of the lemma we will say that A is almost sure if $P(A)\geq 1-n^{-c_1t+c_2}$ where c_1, c_2 depends only on ϵ, ϵ_0, ϵ_1, ϵ_2.

If $g_i(x)$ denotes the 'restriction' of the function $g(x)$ onto the set H_i in the following strong sense: $\mathrm{dom}(g_i)=H_i$ and for all $x\in H_i$, $g_i(x)=g(x)\cap H_i$, and $K_i(x)=\{y\in H_i \mid x\in g_i(y)\}$, then we have that (H0), (H1) and (H2) are almost sure, where

(H0) (a) $|g_0(x)|<t/2$ for all $x_0\in H_0$, and
(b) $|\{x\in H_0 \mid |K_0(x)|>\sqrt{|H_0|}\}|<t/2\sqrt{|H_0|}$.

(H1) $|\{x\in H_1 \mid |K_1(x)|>t/2\}|<t/2$.

(H2) $|\{x\in H_2 \mid K_2(x)\neq 0\}|<t$.

((H2) is equivalent to the asserdon of Lemma 6 with $\delta = \epsilon_2$.)

(H0) (a) follows from (*).

(H0) (b). (H0) (a) implies that $\Sigma_{x \in H_0} |K_0(x)| < t/2\,|H_0|$ which implies (H0) (b).

(H1) follows from (H0) and (*). Indeed, by (*), $|\{x \in H_1 \mid |K_0(x)| > \sqrt{|H|}\}| < t/2$ is almost sure, and again according to (*) for all $x \in H_1$ with $|K_0(x)| < \sqrt{|H|}$, we have that $|K_1(x)| < t/2$ is almost sure.

(H2). Let $H_1' = \{x \in H_1 \mid |K_1(x)| \leqslant t/2\}$. (H1) implies that $|H_1 - H_1'| < t/2$. It is sufficient to prove that $|\{x \in H_2 \cap H_1' \mid K_2(x) \neq 0\}| < t/2$, but this is an immediate consequence of (**) with $t \to t/2$, $Q(x) \to K_1(x)$. □

Lemma 7. *Suppose that $0 < \epsilon < \frac{1}{2}$ and k is a positive integer. Then there exists a $\delta > 0$ such that for any finite set H if g is a function defined on the Cartesian product $\prod_k H$ with $g(x) \subseteq H$, $|g(x)| \leqslant |H|^{1-\epsilon}$, $g(\langle x_0, \ldots, x_{k-1}\rangle) \cap \{x_0, \ldots, x_{k-1}\} = \emptyset$ for all $x = \langle x_0, \ldots, x_{k-1}\rangle \in \prod_k H$ and H' is a random subset of H with $[|H|^{\delta}]$ elements, then for all $t > 0$ we have*

$$P(|\{y \in H' \mid y \in g(x) \text{ for some } x \in \prod_k H'\}| > t) < n^{-c_1 t + c_2}$$

where $c_1 > 0$ and c_1, c_2 depend only on ϵ and k.

Proof. We prove the lemma by induction on k. For all $z \in H$ let g_z be a function with $\mathrm{dom}(g_z) = \prod_{k-1} H$ and $g_z(\langle x_0, \ldots, x_{k-2}\rangle) = g(\langle x_0, \ldots, x_{k-2}, z\rangle)$. Clearly $g_z(\langle x_0, \ldots, x_{k-2}\rangle) \cap \{x_0, \ldots, x_{k-2}\} \subseteq g(\langle x_0, \ldots, x_{k-2}, z\rangle) \cap \{x_0, \ldots, x_{k-2}, z\} = \emptyset$ and $|g_z(x)| \leqslant |H|^{1-\epsilon}$ for all $x \in \prod_{k-1} H$.

Applying the inductive hypothesis for each g_z, if H' is a random subset of H with $[|H|^{\delta'}]$ elements (for some δ' which depends only on ϵ and k) we get

$$(7.1)\quad P\left(\forall z \in H \left|\left\{y \in H' \;\middle|\; \exists x \in \prod_{k-1} H'\, y \in g_z(z)\right\}\right| \leqslant t\right) \geqslant 1 - n^{-c_1 t + c_2}.$$

Let g' be a function defined on H' by $g'(z) = \{y \in H' \mid \exists u \in \prod_{k-1} H'\, y \in g_z(u)\}$.

If the assertion described in (7.1) holds, then $|g'(z)| \leqslant t(k-1)$. Let $\mathrm{Cord}(x) = \{x_0, \ldots, x_j\}$ if $x = \langle x_0, \ldots, x_j\rangle$.

$$g'(z) \subseteq \bigcup_{x \in g_z(u)} \mathrm{Cord}(x) \subseteq \bigcup_{x \in g(\langle u, z\rangle)} \mathrm{Cord}(x) = C,$$

so $C \cap \mathrm{Cord}(\langle x, z\rangle) = 0$ implies $z \notin g'(z)$. Hence, applying Lemma H1 (we may suppose that $|H'|^{1-\epsilon} \geqslant t(k-1)$), we get that if H'' is a random subset of H' with $[|H'|^{\delta''}]$ elements then

$$(7.2)\quad P(|\{y \in H'' \mid \exists x \in H''\, y \in g'(x)\}| \geqslant t) \leqslant n^{-c_3 t + c_4}.$$

Suppose now that $y \in g'(x)$ for some $y \in H''$, $x \in \prod_k H''$. If $x = \langle x_0, \ldots, x_{k-1}, z\rangle$, then $y \in g_z(u)$ for some $z \in H''$ and $u \in \prod_{k-2} H'' \subseteq \prod_{k-2} H'$. That is, $y \in g'(z)$, so (7.2) implies the assertion of the Lemma. □

Now we return to the proof of Lemma 5.

Lemma 8. *Suppose* $r_1, r_2, m_1, m_2, m_3 \in \omega$ *and* $\eta_1 \in \mathrm{fn}(r_1, m_1, m_2)$, $r^{(\eta_1)} = r_2$, $\eta_2 \in \mathrm{fn}(r_2, m_2, m_3)$, $r^{(\eta_2)} = r_3$. *Then there exists an* $\eta \in \mathrm{fn}(r_1, m_1, m_3)$ *with* $r^{(\eta)} = r_3$ *so that for all* $f \in \mathrm{fn}(r_1, m_1)$, f_η *is defined iff both* f_{η_1} *and* $(f_{\eta_1})_{\eta_2}$ *are defined, and in that case* $f_\eta = (f_{\eta_1})_{\eta_2}$. *Moreover, for all* $F \subseteq \mathrm{fn}(r_1, m_1)$, $(F_{\eta_1})_{\eta_2} = F_\eta$. *(The function* η *will be denoted by* $\eta_1 \circ \eta_2$.)

Lemma 8 is an immediate consequence of the definitions and implies the following:

Lemma 9. *If A can be k-reduced to B and B can be k-reduced to C, then A can be k-reduced to C.*

The next lemma is the most important result about k-reducibility.

Lemma 10. *If* Ω *is the relation that holds for every possible* $\langle r, n, F, t\rangle$, *then for all* $k \in \omega$, Ω *can be k-reduced to* $w(F) \leqslant t$.

We prove this lemma by induction on k.

Lemma 11. *The relation* Ω *can be* 1*-reduced to* $w(F) \leqslant t$.

We will use in the proof the following example for a Γ-random variable on $r \times m$.

Example. Let S be an arbitrary subset of m with s elements and Q an arbitrary subset of $r-1$ with q elements and with $0 \notin Q$. For all S and Q, we define a Γ-random variable η on $r \times m$ whose values are in $\mathrm{fn}(r, m, s, q)$.

We define $\eta(\langle i, j\rangle)$ by recursion on i. Assume that $\eta|_{i\times m}$ is already defined so that there is a $h \in \mathrm{fn}(r, m, s, q)$ with $\eta|_{i\times m} = h|_{i\times m}$.

If $i \notin Q$, then let $\eta|_{\{i\}\times m}$ be a random one-to-one map of $\{i\} \times m$ onto $\{i+1\} \times m$ with uniform distribution.

If $i \in Q$, then first let $\bar{S}_i = \{\eta^{i-1}(\langle 0, x\rangle) \mid x \in m - S, \eta^j(\langle 0, x\rangle)$ is defined for all $j = 1, 2, \ldots, i-1\}$.

Now, let $\eta|_{\{i\}\times m}$ be a random one-to-one map of $\bar{S}_i$ into $\{i+1\} \times m$, again with uniform distribution. It is easy to see that η is indeed a Γ-random variable on $r \times m$.

Proof of Lemma 11. Let $F \subseteq \mathrm{fn}(r, m)$, $\|F\| \leqslant 1$. Let $0 < \epsilon < \frac{1}{10}$ be fixed. Put $g(x) = \{f(x) \mid f \in F\}$ for all $x \in r \times m$, $G = \{x \in r \times m \mid |g(x)| \geqslant m^{1-\epsilon}\}$.

Case I: $|G| \geqslant m^{2\epsilon}$. If η is the random variable given in our example with $|S| = [m^\epsilon]$, $|Q| = cr$, then

$$P(\emptyset \in F_\eta) > 1 - (1 - 1/(2m^\epsilon))^{m^{2\epsilon}} > 1 - m^{-m^{\epsilon/2}}.$$

$\emptyset \in F_\eta \to \mathrm{Min}(F_\eta) = \{0\}$ implies that $w(\mathrm{Min}_k(F_\eta)) = 0$ which proves our assertion.

Case II: $|G| < m^{2\epsilon}$. Let η be again the random variable given in the example with $|S| = |m^{\epsilon'}|$ and $Q = (r-1) - \{0\}$ where $\epsilon' < \epsilon/8$. Let $X = (r - \{0\}) \times m - \mathrm{rng}(\eta)$. For all $i \in r - \{0\}$, $X \cap \{i\} \times m$ has a uniform distribution on the subsets of $\{i\} \times m$ with $[m^{\epsilon'}]$ elements. Therefore, there is a random variable Y (defined on the same space as η) so that Y is uniformly distributed on the subsets of $r \times m$ with $[m^{2\epsilon}]$ elements and $P(Y \supseteq X) \geq 1 - m^{-h_1(m)}$ where $\lim_{m\to\infty} h_1(m) = \infty$. (Here we used that m is sufficiently large compared to r.)

Let us apply Lemma 6 with $H \to r \times m$, $H' \to Y$ and $g(x) \to$ (the function defined as $g(x)$ if $x \notin G$ and $\emptyset$ otherwise).

Let $W = \{y \in X \mid \exists x \notin G\, y \in g(x)\}$. If $X \subseteq Y$, then Lemma 6 implies that $P(|W| \geq t) < m^{-h_2(t)}$ where $\lim_{t\to\infty} h_2(t) = \infty$. $|G| < m^{2\epsilon}$ implies that if $X \subseteq Y$, then $P(|G \cap X| \geq t) < m^{-h_3(t)}$, where $\lim_{t\to\infty} h_3(t) = \infty$. The set $(G \cap X)_\eta \cup W_\eta$ covers F_η according to the definition of W and G which proves our assertion. □

Proof of Lemma 10. We prove the lemma by induction on k. For $k = 1$, our assertion is equivalent to Lemma 11. Suppose $k \geq 2$. We will prove the following assertions:

(a) Ω can be k-reduced to $Y(r, m, F, t)$ where

$$Y(r, m, F, t) \equiv \text{“for all } x, y \in r \times m \text{ if } F^{x,y} = \{f \in F \mid f(x) = y\}, \text{ then } w(F^{x,y}) \leq t\text{”}.$$

(b) $Y(r, m, F, t)$ can be k-reduced to $W(r, m, F, t)$ where

$$W(r, m, F, t) \equiv \text{“}w(F) < t\text{”}.$$

Proof of (a). Let $F \subseteq \mathrm{fn}(r, m)$, $\|F\| \leq k$ and $\bar{F}^{x,y} = \{f|_{\mathrm{dom}(f)-\{x\}} \mid f \in F, f(x) = y\}$ for all $x, y \in r \times m$. Clearly, $\|\bar{F}^{x,y}\| \leq k - 1$. Applying the inductive hypothesis, we get a random variable η so that

$$(11.1)\quad P(\forall x, y \in r \times m\; w(\mathrm{Min}_{k-1}(\bar{F}^{x,y})_\eta) \leq t) \geq 1 - m^{-h(t)}$$

where $\lim_{t\to\infty} h(t) = \infty$. (Here we used that $|r \times m| < m^2$.) Suppose now that the value of η is fixed with the property given in (11.1).

Let $u = (R(\eta))(x)$, $v = (R(\eta))(y)$ where $x, y \in r^{(\eta)} \times [m_\epsilon]$. We want to prove that $w((\mathrm{Min}_k(F_\eta)^{x,y})) \leq t + 1$. Obviously

$$(\mathrm{Min}_k(F_\eta))^{x,y} \subseteq \mathrm{Min}_k((F_\eta)^{x,y}) = \{g \cup \langle x, y\rangle \mid g \in \mathrm{Min}_{k-1}(\bar{F}^{u,v})_\eta\};$$

therefore if A covers $\mathrm{Min}_{k-1}(\bar{F}^{u,v})_\eta$ then $A \cup \{x\}$ covers $(\mathrm{Min}_k(F_\eta))^{x,y}$.

Proof of (b). Let η be again the Γ-random variable given in the example where $S = [m^\epsilon]$ and $Q = \{i \in (r-1) \mid i \text{ is even}\}$. Let

$$J = \{\langle u, v\rangle \in r \times m \mid (u < r - 1 \wedge \langle u, v\rangle \notin \mathrm{dom}(\eta)) \vee (u > 0 \wedge \langle u, v\rangle \notin \mathrm{rng}(\eta))\}.$$

The definition of Q implies that $|J \cap (\{i\} \times n)| = [m^\epsilon]$ for all $i \in r$. As in the proof of the previous lemma we may suppose that there is a random variable Y so that $P(Y \supseteq J) \geq 1 - m^{-h_1(m)}$ and Y is uniform on the subsets of $m \times r$ with $[m^{2\epsilon}]$ elements.

We prove that the random variable η satisfies the requirements of (b). Let $F \subseteq \mathrm{fn}(r, m)$, $\|F\| \leq k$ and suppose that for all $x, y \in r \times m$ we have $w(F^{x,y}) \leq t$. We have to prove that

$$P(W(r^{(\eta)}, [m^{\epsilon/2}], \mathrm{Min}_k(F_\eta), t')) \geq 1 - m^{-h'(t)}.$$

Let $H = \{f \in F \mid \langle i, j\rangle \in \mathrm{dom}(f) \to i \text{ is even}\}$. The definition of $\eta|_{\{i\}\times m}$ for odd i's implies that $\mathrm{Min}_k(F_\eta) = \mathrm{Min}_k(H_\eta)$. (According to the definition of k-reducibility, we may suppose that $\|F\| \leq k$.) $w(H^{x,y}) \leq w(F^{x,y}) \leq t$; therefore for all $x, y \in r \times m$ there is a $G(x, y) \subseteq r \times m$ so that $\{x\} \cup G(x, y)$ covers $H^{x,y}$, $|G(x, y)| \leq t$, $x \notin G(x, y)$. The definition of H implies that we may suppose that $y \notin G(x, y)$, that is, $\{x, y\} \cap G(x, y) = 0$. According to Lemma 7, $P(|Z| \geq t') \leq m^{-h(t')}$ where $Z = \{u \in Y \mid u \in G(x, y) \text{ for some } x, y \in Y\}$. We claim that if $Y \supseteq J$, then Z_η covers $\mathrm{Min}_k(F_\eta)$. Indeed, suppose that $f_\eta \in \mathrm{Min}_k(F_\eta)$ and $f_\eta(u') = v'$, since $k \geq 2$, $|f| = k$ there is a $x' \in \mathrm{dom}(f_\eta)$ so that $x' \neq u'$. Suppose $f_\eta(x') = y'$ and $(R(\eta))(x') = x$, $(R(\eta))(y') = y$. We have $f(x) = y$, $f \in H^{x,y}$ so $\{x\} \cup G(x, y)$ covers f, that is, either $u \in G(x, y)$ or $v \in G(x, y)$ where $u = (r(\eta))(u')$, $v = (R(\eta))(v')$. Assume that, e.g., $u \in G(x, y)$, $x, y, u \in J$ implies that $u \in Z$ and therefore $u' \in Z_\eta$. □

Now we prove Lemma 5.

Proof of Lemma 5. This lemma is a consequence of Lemma 10. Using the notation of the definition of reducibility, we prove the lemma by induction on t'. For $t' = 1$, Lemma 11 is equivalent to our assertion.

Suppose $t' > 1$ and that the statement of the lemma holds for $t' - 1$.

Assume that $F \subseteq \mathrm{fn}(r, n)$, $\|F\| \leq t'$. Let η_1 be the random variable guaranteed by Lemma 10 for $k = t'$. For every fixed value of η_1, let $G(\eta_1) = \{f \in F_{\eta_1} \mid \|f\| \leq t' - 1\}$. $\|G(\eta_1)\| \leq t' - 1$. Therefore applying the inductive hypothesis, we get a random variable η_2 so that

$$P(w(\mathrm{Min}((G(\eta_1))_{\eta_2}) \leq t)) \leq 1 - n^{-h(t)}.$$

Let $\eta = \eta_1 \circ \eta_2$. The definition of η_1 and η_2 implies that with a probability greater than $1 - n^{-h(t)}$, we have both $w(\mathrm{Min}_{t'}(F_{\eta_1})) < t$ and $w(\mathrm{Min}((G(\eta_1))_{\eta_2})) \leq t$. $\mathrm{Min}(F_\eta) \subseteq \mathrm{Min}((G(\eta_1))_{\eta_2}) \cup (\mathrm{Min}_{t'}(F_{\eta_1})_{\eta_2})$, therefore, $w(\mathrm{Min}(F_\eta)) \leq 2t$. □

References

[1] M. Ajtai, Σ_1^1-formulae on finite structures, Ann. Pure Appl. Logic 24 (1983) 1–48.

[2] R. Fagin, A spectrum hierarchy, Z. Math. Logik Grundlag. Math. 21 (1975) 123–124.

[3] M. Furst, J.B. Saxe and M. Sipser, Parity circuits and the polynomial time hierarchy, Twenty-second FOCS (1981) 260–270.

[4] N. Immerman, Languages which capture complexity classes, Fifteenth STOC, 347–354.